Data Security - In Field

For employees working with customer data in the field (e.g. Sales, Maintenance teams) Fill in the Data Security Consent Form After Review!

Topics

- Introduction to Data
- GDPR Introduction
- Why is Data Security Important?
- Sensitive Data and PII
- External Data Security
- Internal Data Security

Data

What is data?

What is data?

- **Data** is information that is used for analysis.
- It can be **numerical** (#, %, $) or **textual**.
- Sales Agents collect data from the customer at the point of sale and through the feedback surveys including; customer name, GPS location, size of household, fuels used.
- ACE then stores this data and uses it to measure and improve performance or customer service.
- This data must be collected, stored, and used in a secure way → this is called **data security**.

What will happen to the data I fill in?

- Data is used to make **sales**, conduct **maintenance**, manage **loans**, create **impact measurement** statistics, and secure **financing**.

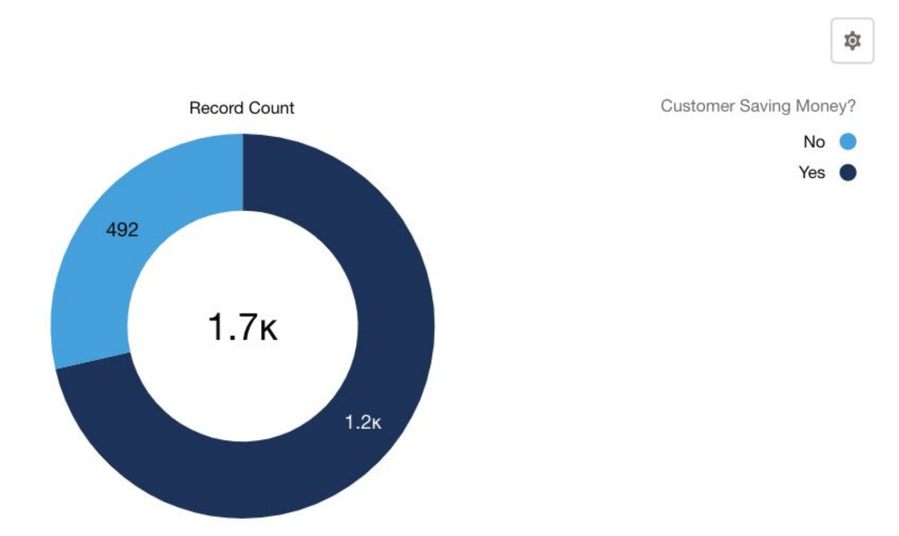
1. Data collected at the **point of sale** is used to conduct maintenance & manage loans.
2. Data collected through **surveys** (on household size, fuel usage, etc.) is used to gain an understanding of the customer demographics to create impact metrics.

Data Journey: from Survey to Metric

- In the Energy Survey, in-field agents collect data on the customer's energy and spending habits. For example, how has your monthly fuel expenditure changed? Are you saving money?
- This data is uploaded directly onto **Salesforce**, where ACE Management can organise this data into **visualisations** and **metrics**.

Data Journey: from Survey to Metric

- The data you fill in gives ACE management an understanding of the customer base.
- Visualisations like this one are used to apply for more loan financing.



Who will see the data I fill in?

The data filled in will be seen by:

1. All ACE employees (in local market & in ACE Amsterdam)
2. Local governments
3. Third parties that ACE partners with
4. Investors

Why is data collection important?

- As in-field agents, the data you fill in from **sales, cases, and surveys** forms the backbone of all of **ACE's operations**!

- It is crucial that the data is filled in **completely** and **accurately.**
- If data is **missing** → this will worsen customer service & prevent ACE from securing financing.
- If data is **inaccurate** → this may lead to legal difficulties.

GDPR Principles

To protect data at ACE

GDPR Principles

- GDPR stands for **General Data Protection Regulations**
- It is a **Pan-European** data protection law that exists to enforce data security measures.
- GDPR applies to all ACE Markets because data is processed through Amsterdam
- GDPR issues fines when broken by the organisation, therefore it is important that all employees follow certain data security policies.
- This presentation will introduce you to data security measures you must take when handling data to comply with GDPR.

Data Security

Introduction

What is Data Security?

- Data security is concerned with the **protection of personal data.** This includes unauthorized access, processing, and damage to this data.

1. You need to keep your data secure from **external threats,** such as hackers.
2. You also need to keep your data secure from **within your organisation** by putting in place guidelines for collecting, storing, and using data.

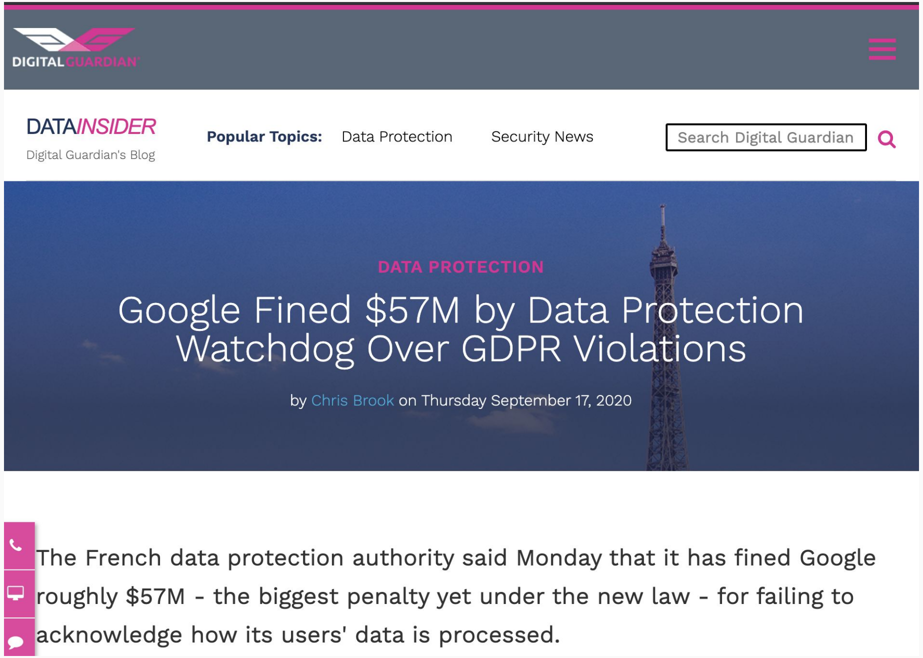
Why is it important?

1. The GDPR has strict **fines** for when data security is not maintained (up to 2% of a company's annual revenue)

2. Data breaches have consequences for the **wellbeing of customers**

3. Data breaches have consequences for the **reputation of ACE**

GDPR Fines in the News



DIGITAL GUARDIAN

DATA*INSIDER*

Digital Guardian's Blog

Popular Topics: Data Protection Security News

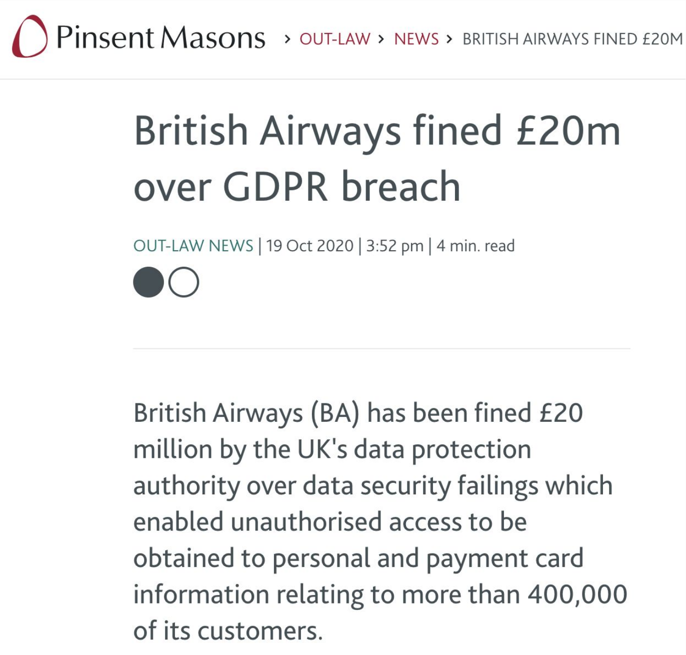
Search Digital Guardian

DATA PROTECTION

Google Fined $57M by Data Protection Watchdog Over GDPR Violations

by Chris Brook on Thursday September 17, 2020

The French data protection authority said Monday that it has fined Google roughly $57M - the biggest penalty yet under the new law - for failing to acknowledge how its users' data is processed.



Pinsent Masons › OUT-LAW › NEWS › BRITISH AIRWAYS FINED £20M

British Airways fined £20m over GDPR breach

OUT-LAW NEWS | 19 Oct 2020 | 3:52 pm | 4 min. read

British Airways (BA) has been fined £20 million by the UK's data protection authority over data security failings which enabled unauthorised access to be obtained to personal and payment card information relating to more than 400,000 of its customers.

Data Security for Customers

- When ACE sells their products to new individuals, it begins a customer relationship: this relationship is built on **trust**.
- Customers can expect ACE to manage their data in a responsible manner.
- If ACE does not uphold external and internal data security, it will break customer trust.
- This can negatively affect the customers, as their sensitive information can land in the hands of those with **malicious intent**.
- Consequently, **ACE's reputation will be damaged by word of mouth**. This will have a negative impact on future sales.

Sensitive Data & PII

Gaining Customer Trust

Sensitive Data

1. Some of the data that ACE collects from customers is **sensitive**.
   - Examples of sensitive data are:
     - Loan Status
     - Amount in Arrears
     - Payment History
   - This data is used to conduct business: sell ACE ones, manage loans.
   - Sensitive data is information that must be protected.

Personally Identifiable Information (PII)

2. **Personally Identifiable Information (PII)** is another type of data that is used to uniquely identify a specific individual or customer.

- PII Examples are:
  - Full Name
  - Phone Number
  - Location
  - Social Security Number
- ACE collects this data to service customers.

Combining Sensitive Data & PII

- When you **combine sensitive data with PII**, this can be used to tie particular behaviors to individuals.
- For example: you know John Smith’s full name, phone number, and the fact that he has 30EUR remaining balance on his loan.
- This is information that may cause dangerous situations for the customer.
- Therefore, you should take some steps to ensure you are protecting this data.

Protecting Data

1. Confirm whether you are dealing with a combination of sensitive data & PII by following this checklist.
2. If yes, **do not share this data outside of ACE** without explicit permission or instructions.
3. If you are sharing within ACE, assess whether you need to include PII in your message. If it is not necessary, perhaps remove it from your message.
4. If you must include PII in your message to accomplish your goal, you should follow steps to keep your phone secure (see the external data security steps later in this presentation)

Protecting Data

- Remember that the steps in this presentation exist to keep customer data safe, but there may be times where you cannot remove PII from your messages.
- We simply ask you to consider the principles of data security & the sensitivity of data when using or sharing this data.

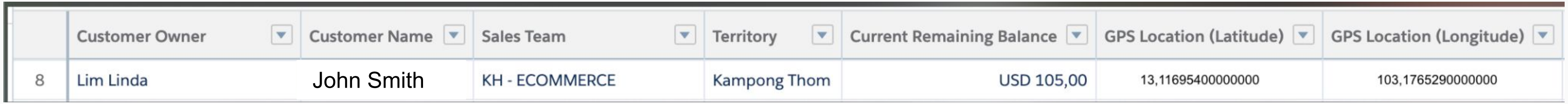
Checklist: is this PII?

You can use this checklist to determine whether the data you are looking at contains PII.

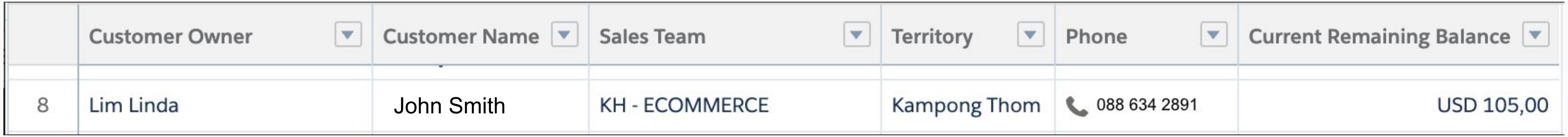
- ❏ Does this piece of information **identify an individual customer** or can it apply to more than one customer?
  - ❏ Example: GPS coordinates of a customer’s house vs. territory
- ❏ If this information is shared out of ACE, could external parties **locate or contact the customer**?

If YES, then it is PII.

Quiz: What is the PII?

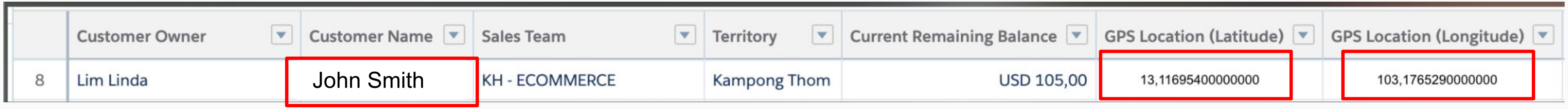


	Customer Owner	Customer Name	Sales Team	Territory	Current Remaining Balance	GPS Location (Latitude)	GPS Location (Longitude)
8	Lim Linda	John Smith	KH - ECOMMERCE	Kampong Thom	USD 105,00	13,11695400000000	103,1765290000000



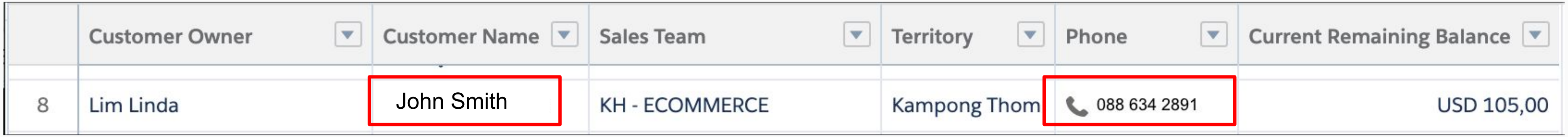
	Customer Owner	Customer Name	Sales Team	Territory	Phone	Current Remaining Balance
8	Lim Linda	John Smith	KH - ECOMMERCE	Kampong Thom	☎ 088 634 2891	USD 105,00

Examples of Personally Identifiable Information



	Customer Owner	Customer Name	Sales Team	Territory	Current Remaining Balance	GPS Location (Latitude)	GPS Location (Longitude)
8	Lim Linda	John Smith	KH - ECOMMERCE	Kampong Thom	USD 105,00	13,11695400000000	103,1765290000000

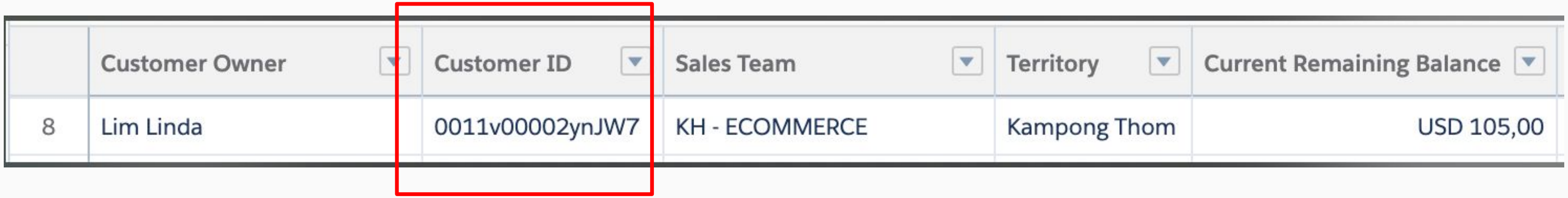
Personally Identifiable Information



	Customer Owner	Customer Name	Sales Team	Territory	Phone	Current Remaining Balance
8	Lim Linda	John Smith	KH - ECOMMERCE	Kampong Thom	☎ 088 634 2891	USD 105,00

PII and Customer IDs

- To protect the customer’s sensitive data, ACE assigns a unique **Customer ID** to every customer that can replace PII.
- This unique ID can be used to create reports and share data on sales, service, and loan management with third parties.
- Now, if third parties get a hold of the data, they cannot tie this record to an individual customer.



	Customer Owner	Customer ID	Sales Team	Territory	Current Remaining Balance
8	Lim Linda	0011v00002ynJW7	KH - ECOMMERCE	Kampong Thom	USD 105,00

Customer Trust

- By replacing PII, like a full name, with a unique Customer ID when sharing or working with data, ACE will protect the sensitive information of customers.
- If you have the opportunity to replace PII with a Customer ID, you should do so.
- This gains **customer trust** and **customer safety**.

ACE Employee Data

- ACE also stores data on its **employees**, for example: contact information, role, payroll information, etc.
- This **HR data** should also be handled with care.
- When accessing, using, and sharing this data → make sure to apply the data security principles in this presentation.

External Data Security

How do we protect data against external threats?

What is External Data Security?

- External data security refers to measures to protect data from **external threats** such as hackers, or unauthorized access.
- External data security measures are taken by all ACE employees in all of the markets.

Some examples include: ACE uses very secure applications to store data, ACE requires users to log-in before accessing data, ACE puts in place security measures on the customer-facing applications.

Data on ACE Platforms

- ACE stores data on two different platforms: **G-Suite and Salesforce**.
- When you fill in data on your **tablet**, this is automatically sent to these platforms.
- These are very **secure platforms** that have their own data security measures in place.

External Data Security for In-Field Agents

- As in-field agents, there are some steps you should take to keep customer data secure from external threats.
- They will be related to **how and where you store your data.**
- Since you collect and access data in-field, you are responsible for making sure that you manage this data with care.

External Data Security for In-Field Agents

1. Install a **password** on your phone or tablet.
2. Do not share your TaroWorks account with people that should not have access to this account.
3. Use only **work devices** to access ACE data (unless it is absolutely necessary to use your own device).
4. Before sending customer data on WhatsApp, evaluate whether you can remove PII from the message.

Password Requirements

- ❑ Passwords for your ACE accounts should be difficult to guess.
- ❑ For example, include both **lowercase and UPPERCASE** letters, include **numbers**, and **special characters** (!@#$%^).
- ❑ It is very important to keep your passwords **private**, if you have trouble remembering your passwords you can write them down in a secret location.
- ❑ If you have the ability to do so, your password should be **updated** every 4 months.

Internal Data Security

Internal company policies

What is internal data security?

- Internal data security is concerned with the **collection, storage, access, usage, and sharing** of data within the organisation.
- Different roles within ACE require access to different data.
    - Sales Manager need information on demos, prospects, and well-performing sales teams
    - Call Center agents need to know the phone numbers of different customers
- Data sometimes has to be **shared** across countries or departments to complete activities → this needs to be done in a secure way.
- Internal data security also relates closely to data privacy.

What is Internal Data Security?

- Internal data security is concerned with the **collection, storage, access, usage, and sharing** of data within the organisation.
- Different roles within ACE require access to different data.
- Data sometimes has to be **shared** across countries or departments to complete activities → this needs to be done in a secure way.
- For in-field agents, the most important concept in internal data security is **communication.**

General Communication

- Every market has their own best practices when it comes to communication: WhatsApp, Gmail, Google Chat, etc.
- Communication at ACE can include discussing sensitive information of customers or employees (customer names, loan status, etc.)
- Therefore, when sharing or discussing sensitive customer/employee data, you must use the **G-Suite tools (Gmail & Google Chat)** whenever possible, as this communication is secured.
- If you do not have access to the G-Suite tools, you may use your preferred method of communication (WhatsApp)

If you are in doubt… Ask!

- Are you sharing sensitive data?
- Is someone asking you to share data you believe is sensitive?
- Is someone asking you to share your login details?
- Are you unsure who should have access to your tablet or phone?
- Any confusion about data security?

Next Steps - Fill in the form!

- Please take the time to fill out this form where you consent to reading and understanding the information in this presentation.
- Access the form by clicking here